Lashanti Gladney

Policy Analysis

09/29/24

The Cybersecurity Information Sharing Act

The rise of technologies has created new ways for criminals to exploit user data, which is why cybersecurity is more important than ever. Struggles with maintaining cybersecurity has been an issue seen not only in company breaches such as Target and Equifax but with the government as well. The creation of acts such as the Cybersecurity Information Sharing Act (CISA) as well as the Foreign Intelligence Surveillance Act (FISA) were meant to aid in combatting these issues. I'll be going into more detail about what these acts cover as well as a few programs that played a factor in their creation, PRISM, and XKeyscore and the Five Eyes Alliance.

The Cybersecurity Information Sharing Act furthermore known as CISA was created by the United States Congress in 2015 that opens collaboration between the government as well as companies to share information about security breaches. There is a saying that you must know your enemy to defeat them, this act would aid in this. By sharing information new techniques can be implemented to strengthen cybersecurity both public and private. This sharing of information was done using Automated Indicator Sharing, also known as AIS, which was developed by the Department of Homeland Security to exchange information of cyberthreats. This is unique because AIS does this in real time, the system is also able to get rid of malware signatures and other malicious software on its own. This aids in the amount of time needed to counter cyber attacks and without the direct need for human intervention. AIS is not perfect however, there are still some drawbacks to the program. There is a chance that sensitive information could be shared in the process of sharing information about cyber incidents. This is an issue when it comes to most companies in terms of how user data is being shared and if there are proper protocols in place to protect this data. There is also a chance that some valuable security information could be overlooked by the program due to the large amounts of data constantly going though the system, making it possible for some malicious software to get through. Overall, the positives still far outweigh the negatives, as in the world of cyber there is no system without fault.

The Foreign Intelligence Surveillance Act (FISA) was created long before CISA back in 1978 with the purpose of regulating foreign intelligence. In the event the government was to face some form of cyber-attack or cyber terrorism the FBI can counter them without having to compromise the rights of U.S. citizens. As I mentioned before what is done with personal data continues to be a big concern amongst the people regardless of the country. This is why clauses meant to protect citizens privacy and personal information is more is essential although there are still some concerns. For example, there is a section that gives permission to the National Security

Agency (NSA) to collect foreign intelligence information as well. The negative of this came with the NSA also collecting information from U.S. citizens. This alarmed citizens, as they became worried about what types of information was being collected and how citizens were being tracked. This information ranged from social media activity, locations, and even financial information. Operating under the NSA the Planning Tool for Resource Integration, Synchronization, and Management or PRISM, collects online information from major companies such as Google and Microsoft in the name of national security. The concern with the citizens like their issue with FISA was the types of information being gathered, PRISM, was allowed to collect data from emails, messages, photos, and other information that could be seen online. This became a problem as it began to make citizens question what information they have that is unmonitored, with so much personal information online it can be unsettling knowing that your data is being monitored and possibly vulnerable to being exploited. Another NSA surveillance program is XKeyscore, a program that allows the pulling of information from any data found on the internet, with no need to gather information from companies in the manner that PRISM does. This is what tracks everything that a citizen searches online, search history, Ip addresses, essentially anything a person does online can be tracked back with XKeyscore. These various programs eliminate any form of information friction between the government and its citizens with their being no real privacy online.

To go even further in terms of surveillance there is the Five Eyes Alliance which is an agreement of information sharing between the United States, the United Kingdom, Canada, Australia and New Zealand. The information being collected from the programs XKeyscore, and PRISM being shared has been even more controversial, countries collecting endless amounts of data and sharing it among themselves, begs the question if it was all in the name of security or for some form of other gain. This alliance started as an alliance to share information in the traditional military sense, but as time has gone on and more has turned to digital, even warfare, this alliance has adapted to do the same. At its core the information being shared is helpful with countries working together to identity threats and gather intel that could help further the cybersecurity measures used in other countries. Just as how when gathering information with PRISM or sharing with CISA there is always a chance for personal information to be mixed in and shared along with information strictly for intelligence.

Overall, there are various acts and programs that feeds into the Cybersecurity Information Sharing Act. FISA, PRISM, XKeyscore, and the Five Eyes Alliance all collect various types of information that can then be shared rather that comes in the form of companies and the government or the U.S. government with other countries. The sharing of this information it boils down to being in the name of cybersecurity, which this is accomplished, although not without some concern. Between the programs I have mentioned information such as browsing history, emails, financial information, as well as information from big companies such as Google or Microsoft. These companied contain endless amount of personal data which if exploited could greatly affect the lives of many however this is a possible consequence to having any information

being stored online. The benefits of these programs must continuously outweigh the potential loss, as we continue to evolve in terms of technology in the future there will likely be more programs developed to monitor and combat against cyber threats as well as acts to protect the information of citizens.

References

Brad Williams. "*Why the Five Eyes? Power and Identity in the Formation of a Multilateral Intelligence Grouping."* Journal of Cold War Studies, vol. 25, no. 1, 2023, pp. 101-137. doi: https://doi.org/10.1162/jcws_a_01123.

Conti, Gregory, and David Raymond. *"Ethical Cyber Operations: The Human Factor in Cybersecurity."* Journal of Information Warfare, vol. 16, no. 1, 2017, pp. 24-37.

FBI. *"FBI Releases FISA Query Guidance."* FBI.gov, 2023, https://www.fbi.gov/news/press-releases/fbi-releases-fisa-query-guidance.

Karp, Ben. *"Federal Guidance on the Cybersecurity Information Sharing Act of 2015."* The Harvard Law School Forum on Corporate Governance, 3 Mar. 2016, https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/.

Landau, Susan. *"Cybersecurity: Time for a New Security Model."* Harvard Law & Policy Review, vol. 10, no. 2, 2016, pp. 391-428.

Mayer, Jonathan R. *"The Interplay of Technology, Privacy, and Policy in Cybersecurity Information Sharing."* Yale Law & Policy Review, vol. 34, no. 2, 2015, pp. 183-222.

Osaji, Patrick. *"Pros and Cons of the Cybersecurity Information Sharing Act of 2015."* ACE, 2023, https://ace-usa.org/blog/research/research-technology/pros-and-cons-of-the-cybersecurity-information-sharing-act-of-2015/.

White, G. *"Automated Indicator Sharing (AIS): A Real-Time Exchange of Cybersecurity Information."* Journal of Cybersecurity, vol. 9, no. 3, 2020, pp. 213-229.